United States District Court
District of New Jersey

UNITED STATES OF AMERICA	:	Hon. James B. Clark, III
	:	
v.	:	Mag. No. 24-12241
	:	
DANIEL RHYNE	:	**CRIMINAL COMPLAINT**

I, Timothy Lee, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

Timothy Lee
Timothy Lee, Special Agent
Federal Bureau of Investigation

Special Agent Lee attested to this Complaint by telephone pursuant to FRCP 4.1(b)(2)(A).

Sworn to before me and subscribed in my presence,
on August 8, 2024 at Newark, New Jersey

Honorable James B. Clark, III
United States Magistrate Judge

The Hon. James B. Clark, III
Signature of Judicial Officer

ATTACHMENT A

Count One
(Extortion in Relation to a Threat to Cause Damage to a Protected Computer)

On or about November 25, 2023, in Somerset County, in the District of New Jersey and elsewhere, defendant

DANIEL RHYNE

with intent to extort from any person any money and thing of value, did transmit in interstate or foreign commerce any communication containing a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

In violation of Title 18, United States Code, Sections 1030(a)(7)(A) and (c)(3)(A).

Count Two
(Intentional Damage to a Protected Computer)

From on or about November 8, 2023 through on or about November 25, 2023, in Somerset County, in the District of New Jersey and elsewhere, defendant

DANIEL RHYNE

did knowingly cause the transmission of a program, information, code, and, command, and as a result of such conduct, intentionally cause damage without authorization, to a protected computer, and cause loss to Victim-1 during a 1-year period aggregating at least $5,000 in value.

In violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i).

Count Three
(Wire Fraud)

On or about November 25, 2023, in Somerset County, in the District of New Jersey and elsewhere, defendant

DANIEL RHYNE

did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud Victim-1 and to obtain money and property from Victim-1 by means of materially false and fraudulent pretenses, representations and promises, and, for purposes of executing and attempting to execute such scheme and artifice to defraud, did knowingly and intentionally transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, pictures and sounds.

In violation of Title 18, United States Code, Section 1343.

ATTACHMENT B

I, Timothy Lee, am a Special Agent with the Federal Bureau of Investigation ("FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and photographs of the evidence. Where statements of others are related herein, they are related in substance and part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

I. Background and Relevant Terms

1. Victim-1 is a U.S.-based industrial company, with its headquarters located in Somerset County, New Jersey. Victim-1 provides services to various industries, including aquaculture, biopharmaceuticals, chemistry, electronics, food and beverage, healthcare, hydrogen mobility, manufacturing and industrial processing, metals, oil and gas, and pulp and paper companies.

2. The defendant, Daniel Rhyne ("RHYNE") was a resident of Warren County, New Jersey and was employed by Victim-1 as a core infrastructure engineer. As a core infrastructure engineer, RHYNE served as Victim-1's subject matter expert on hosting virtual machines.

3. A "virtual machine" is software that virtually emulates a physical computer. It can perform almost all the same functions as a physical computer. For example, a virtual machine can maintain an operating system with applications and programs.

4. A "domain controller" is a computer server that authenticates and validates user access on a computer network.

5. A "domain administrator" is a user account that has certain administrative privileges, such as the ability to make changes to policies that can impact all computers and/or users within an organization.

6. A "local administrator" is a user account that has certain administrative privileges in a single system within an organization.

7. A "workstation" is a high-performance computer built for professional tasks with more power than a typical desktop computer.

8. A "scheduled task," a/k/a "task scheduler" is a utility in the Microsoft Windows operating system that launches scheduled computer programs at

predefined times.

9. "Net user" is a Microsoft Windows tool that allows the modification of user accounts, including changing passwords and removing accounts.

10. "Sysinternals Utilities" or "Sysinternals" is a collection of tools for computer system administration that allow the user to manage, monitor, and troubleshoot Windows systems. "PsPasswd" is a certain Sysinternals tool that allows for the changing of account passwords on local or remote systems.

11. A "remote desktop" is a program that allows a user to connect to a computer in another location, see that computer's desktop, and interact with it as if the user was locally connected to the network.

II. The Intrusion and the Extortion E-mail

12. On or about November 25, 2023, at approximately 4:00 p.m. EST, network administrators employed at Victim-1 began receiving password reset notifications for a Victim-1 domain administrator account, as well as hundreds of Victim-1 user accounts. Shortly thereafter, the Victim-1 network administrators discovered that all other Victim-1 domain administrator accounts were deleted, thereby denying domain administrator access to Victim-1's computer networks.

13. Approximately 44 minutes later, at 4:44 p.m. EST, certain Victim-1 employees were sent an e-mail from an external, non-employee e-mail address (the "Extortion E-Mail Address") with the subject line, "Your Network Has Been Penetrated" (the "Extortion E-Mail").

14. The Extortion E-Mail warned its recipients (1) that all of Victim-1's "IT administrators ha[d] been locked out or deleted" from Victim-1's computer network; (2) that all of Victim-1's "backups ha[d] been deleted;" and (3) that an additional "40 random servers w[ould] be shut down each day for [a period of] 10 days" if a ransom of €700,000 euros ("EUR") in the form of 20 bitcoin ("BTC") w[as] not transferred by December 2, 2023 to a BTC address specified in the Extortion E-Mail. On November 25, 2023, 20 BTC had an equivalent value of approximately $750,000.

15. Based on this investigation, law enforcement confirmed that certain malicious activity was conducted on Victim-1's computer network from on or about November 8, 2023 through on or about November 25, 2023 – the date of the Extortion E-Mail. For example, a review of Victim-1's network revealed that there were scheduled tasks on Victim-1's domain controller scheduled to (1) delete 13 Victim-1 domain administrator accounts; (2) change passwords to 301 Victim-1 domain user accounts; (3) change passwords to two Victim-1 local administrator accounts that would impact 254 Victim-1 servers; (4) change passwords to two Victim-1 local

administrator accounts that would impact 3,284 Victim-1 workstations; and (5) shut down several Victim-1 servers and workstations over the course of several days in December 2023. By changing administrator and user passwords and shutting down Victim-1's servers, the scheduled tasks were collectively designed and intended to deny Victim-1 access to its systems and data.

16. As set forth below, this investigation identified RHYNE as the sender of the Extortion E-mail. Additionally, the investigation revealed that RHYNE was responsible for the malicious activity conducted on Victim-1's network, as described above.

III. Identification of RHYNE

Malicious Activity on Victim-1's Domain Controller

17. On or about November 25, 2023, starting at approximately 8:12 a.m. EST, a legitimate Victim-1 domain administrator account (the "Victim-1 Administrator Account") created approximately 16 unauthorized "scheduled tasks" on Victim-1's domain controller. Six of the "scheduled tasks" were configured to execute at specific times on November 25, 2023, starting at 4:00 p.m. EST, to perform the following unauthorized actions on Victim-1's computer network:

- delete 13 Victim-1 domain administrator accounts and change the password of the Victim-1 Administrator Account to, "TheFr0zenCrew!" using the "net user" command tool;
- change the password to 301 Victim-1 domain user accounts to "TheFr0zenCrew!" using the "net user" command tool;
- change the password to two Victim-1 local administrator accounts that would impact 254 Victim-1 servers using the Sysinternals tool "PsPasswd";
- change the password to two Victim-1 local administrator accounts that would impact 3,284 Victim-1 workstations using the Sysinternals tool "PsPasswd."

18. The remaining scheduled tasks were configured to shut down dozens of Victim-1 computer servers over the course of several days starting on December 3, 2023. As set forth previously, if executed, the scheduled tasks would have denied Victim-1 access to its systems and data, which could have interrupted its business operations.

Remote Desktop Session Traced to Hidden Virtual Machine

19. Analysis of Victim-1's computer network revealed that on or about November 25, 2023, at approximately 7:48 a.m. EST, there was an unauthorized

access of the Victim-1 Administrator Account on Victim-1's domain controller that was initiated from a remote desktop session. The remote desktop session continued from approximately 7:48 a.m. EST until approximately 9:45 a.m. EST, during which time the above-described "scheduled tasks" were created.

20. Through its analysis of Victim-1's network, law enforcement learned that the remote desktop session originated from an unauthorized virtual machine on Victim-1's network (the "Hidden Virtual Machine").

21. Further investigation revealed that the Hidden Virtual Machine had been used to access the Victim-1 Administrator Account on Victim-1's domain controller on numerous occasions from on or about November 10, 2023 through on or about November 25, 2023. Additionally, the Hidden Virtual Machine was the only system that conducted a remote desktop session to access the Victim-1 Administrator Account on Victim-1's domain controller during that time-period.

Additional Malicious Activities Conducted from the Hidden Virtual Machine

22. Additional forensic analysis of Victim-1's computer network revealed that the user of the Hidden Virtual Machine prepared for and conducted certain malicious activity on Victim-1's computer network. For example:

a. On or about November 15, 2023, the user of the Hidden Virtual Machine placed Sysinternals Utilities onto Victim-1's domain controller, which included the "PsPasswd" tool that was later used to change various Victim-1 administrator and user passwords, as described above.

b. On or about November 22, 2023, the user of the Hidden Virtual Machine conducted numerous web searches that were related to the above-described malicious activities, which included the following::

- "How to set domain user password from command line"
- "how to delete a dmoain [sic] account from the command line"
- "how to remotely shutdown a computer using cmd"
- "how to clear all windows logs from command line"
- "net user syntax change password"

Hidden Virtual Machine Accessed from RHYNE's Account and Laptop

23. Further forensic analysis revealed that the Hidden Virtual Machine was created on Victim-1's network on or about November 9, 2023, at which time the password for the Hidden Virtual Machine's user account was set to "TheFr0zenCrew!". This password was identical to the changed password of the Victim-1 Administrator Account, as well as the changed password of 301 Victim-1

domain user accounts, as described above.

24. As part of an internal investigation following the incident, certain Victim-1 employees learned that the Hidden Virtual Machine was accessed by the user account and laptop assigned by Victim-1 to RHYNE (the "RHYNE User Account") (the "RHYNE Laptop") for RHYNE's duties as Victim-1's core infrastructure engineer.

25. Additionally, an analysis of the RHYNE Laptop and the Hidden Virtual Machine revealed that from on or about November 9, 2023 through on or about November 25, 2023, all internet browsing activity on the RHYNE Laptop would cease when internet browsing was occurring on the Hidden Virtual Machine. Based on that activity, there is reason to believe that the same user was utilizing the RHYNE Laptop and the Hidden Virtual Machine.

26. Moreover, on or about November 15, 2023, the RHYNE User Account, while logged into the RHYNE Laptop, conducted numerous web searches that were similar to the web searches that were later conducted from the Hidden Virtual Machine on November 22, 2023, as described above. Specifically, the search queries included:

- "command line to change password"
- "command line to change local administrator password"
- "net user"
- "command line to remotely change local administrator password"

27. At relevant times, Victim-1's security cameras and physical access logs recorded RHYNE physically entering Victim-1's headquarters. A review of the security footage and access logs revealed that RHYNE's physical access to Victim-1's headquarters immediately preceded the RHYNE User Account logging into the RHYNE Laptop and, in many instances, the RHYNE User Account subsequently accessing the Hidden Virtual Machine. For example:

a. On or about November 9, 2023, at approximately 6:55 a.m. EST, RHYNE entered Victim-1's headquarters. Approximately three minutes later, at 6:58 a.m. EST, the RHYNE User Account logged into the RHYNE Laptop. Then, at approximately 7:38 a.m. EST, the user of RHYNE Laptop accessed a company spreadsheet with passwords, including the password for the Victim-1 Administrator Account.

b. On or about November 14, 2023, RHYNE entered Victim-1's headquarters at approximately 7:05 a.m. EST. Two minutes later, at approximately 7:07 a.m. EST, the RHYNE User Account logged

into the RHYNE Laptop. At approximately 7:55 a.m. EST, the RHYNE User Account and the RHYNE Laptop accessed the Hidden Virtual Machine.

c. On or about November 21, 2023, RHYNE entered Victim-1's headquarters at 6:54 a.m. EST. Three minutes later, at approximately 6:57 a.m. EST, the RHYNE User Account logged into the RHYNE Laptop. At 9:14 a.m. EST, the RHYNE User Account accessed the Hidden Virtual Machine.

28. Further, analysis of RHYNE'S activities revealed that when RHNYE was not physically present at Victim-1's headquarters, the user of the RHYNE Laptop accessed Victim-1's computer network, including the Hidden Virtual Machine, remotely from an Internet Protocol ("IP") address that was assigned to RHYNE's residence in Warren County, New Jersey (the "RHYNE IP Address"). For example:

a. On or about November 23, 2023, at approximately 6:48 a.m. EST, the RHYNE User Account logged into the RHYNE Laptop. Then, at 6:50 a.m. EST, the RHYNE Laptop connected to Victim-1's network from the RHYNE's IP Address. This gave the user of the RHYNE User Account access to Victim-1's computer network from RHYNE's residence. At 6:57 a.m. EST, the RHYNE User Account then accessed the Hidden Virtual Machine. At 7:02 a.m. EST, there was a remote desktop connection from the Hidden Virtual Machine to the Victim-1 Administrator Account on Victim-1's domain controller.

b. On or about November 25, 2023, at approximately 7:04 a.m. EST, the RHYNE User Account logged into the RHYNE Laptop. Approximately two minutes later, at 7:06 a.m. EST, the RHYNE Laptop connected to Victim-1's network from the RHYNE IP Address. At approximately 7:10 a.m. EST, the RHYNE User Account accessed the Hidden Virtual Machine. At 7:48 a.m. EST, there was a remote desktop connection from the Hidden Virtual Machine to the Victim-1 Administrator Account on Victim-1's domain controller. The Victim-1 Administrator Account then created the previously described "scheduled tasks" that would disrupt Victim-1's computer network, including the changing of passwords of certain Victim-1 domain user accounts.

"TheFr0zenCrew!"

29. During its investigation, law enforcement learned that the password to the Extortion E-Mail Address, which had sent the Extortion E-Mail to Victim-1's

employees on November 25, 2023 was "TheFr0zenCrew!" – identical to the passwords of the Hidden Virtual Machine as well as Victim-1's domain user accounts.

30. Based on this information and the information contained herein, there is probable cause that RHYNE (1) controlled and accessed the Hidden Virtual Machine, which was used to access Victim-1's computer network without authorization and schedule certain tasks designed to disrupt Victim-1's network; and (2) controlled and used the Extortion E-Mail Address, which was used to send the Extortion Email to Victim-1 employees.